PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-098774
(43)Date of publication of application : 14.04.1998

(51)Int.Cl. H04Q 7/38
H04Q 7/34

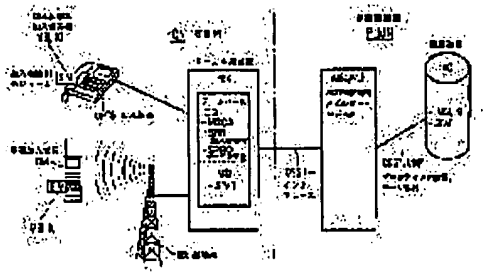
(21)Application number : 09-205859
(22)Date of filing : 31.07.1997

(71)Applicant : SIEMENS AG
(72)Inventor : LINDER HERMANN DIPL ING

(30)Priority
Priority number : 96 19630920 Priority date : 31.07.1996 Priority country : DE

(54) METHOD AND DEVICE FOR AUTHENTICATING SUBSCRIBER AND/OR CODING INFORMATION

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method and a device for subscriber authentication which enable a protecting means to be used at cost as low as possible even in another communication network connected to a mobile radio network respectively.
SOLUTION: The method and device are for authenticating a subscriber and/or coding information, a mobile radio network (PLMN) for a subscriber of another communication network(CN) prepares protection parameters (SPAR) through an interface (DSS1+) connecting both communication networks, and a subscriber of the mobile radio network needs not registers itself in at least one subscriber data base(DB) of the mobile radio network. At this time, the subscriber of the other communication network is identified by a subscriber identification module(SIM) of a subscriber station (UPTD, DM) and recorded in the subscriber data base of the other communication network. Protection parameters for a subscriber recorded in a leased network are requested through an interface, prepared by an authentication device (AC) of the mobile radio network, and transmitted to the leased network through the interface.



LEGAL STATUS
[Date of request for examination] 31.07.1997
[Date of sending the examiner's decision of rejection] 16.05.2000
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平10－98774

(43)公開日　平成10年(1998)４月14日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26		１０９Ｓ
7/34		Ｈ０４Ｑ　7/04		Ｃ

審査請求　有　　請求項の数８　ＯＬ　（全７頁）

(21)出願番号　特願平9－205859

(22)出願日　平成９年(1997)７月31日

(31)優先権主張番号　１９６３０９２０．４

(32)優先日　1996年７月31日

(33)優先権主張国　ドイツ（ＤＥ）

(71)出願人　396026260
ジーメンス　アクティエンゲゼルシャフト
ドイツ　ミュンヘン　Ｄ－80333　ヴィッテルスバッヒャープラッツ　2

(72)発明者　ヘルマン　リンダー
オーストリア　ドルフェン　84405　ジョセフマーティン　バウアー　ストラッセ

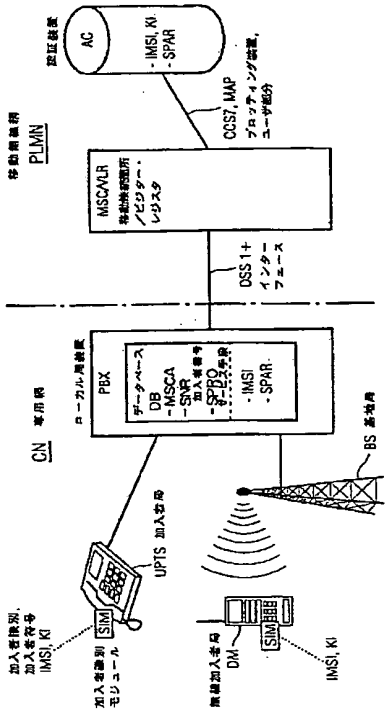
(74)代理人　弁理士　萩原　誠

(54)【発明の名称】　加入者を認証するための及び／又は情報をコード化するための方法及び装置

(57)【要約】

【課題】　保護手段が、それぞれ移動無線網に接続された別の通信網においても可能な限りわずかなコストで使用することの出来る加入者認証方法及び装置を提供する。

【解決手段】　加入者を認証するための及び／又は情報をコード化するための方法及び装置であって、保護パラメータ（ＳＰＡＲ）が別の通信網（ＣＮ）の加入者のための移動無線網（ＰＬＭＮ）によって両通信網を接続しているインターフェース（ＤＳＳ１＋）を介し準備されており、しかも移動無線網の加入者は、移動無線網の少なくとも１つの加入者データベース（ＤＢ）に加入者記録をする必要がない。その際別の通信網の加入者は、加入者局（ＵＰＴＳ，ＤＭ）の加入者識別モジュール（ＳＩＭ）によって識別され、かつ別の通信網の加入者データベースに記録される。専用網に記録された加入者のための保護パラメータは、インターフェースを介して要求され、移動無線網の認証装置（ＡＣ）によって準備されかつインターフェースを介して専用網に伝送される。



1

【特許請求の範囲】

【請求項１】　加入者を認証するための及び／又は情報をコード化するための方法であって、

移動加入者が、移動無線網（ＰＬＭＮ）に対し加入者局に含まれる加入者識別モジュール（ＳＩＭ）によって識別されかつ移動無線網（ＰＬＭＮ）の少なくとも１つの加入者データベースで処理されて認証装置（ＡＣ）に登録されており、該認証装置（ＡＣ）から加入者データを保護するため、移動加入者に対しそれぞれ保護パラメータ及び保護アルゴリズムが準備されている形式のものにおいて、

－インターフェース（ＤＳＳ１＋）を介し移動無線網（ＰＬＭＮ）に接続された別の通信網の加入者を、加入者識別モジュール（ＳＩＭ）によって識別しかつ少なくとも別の通信網（ＣＮ）の加入者データベース（ＤＢ）で処理し、

－別の通信網（ＣＮ）の処理された加入者のための保護パラメータ（ＳＰＡＲ）をインターフェース（ＤＳＳ１＋）を介して要求し、移動無線網（ＰＬＭＮ）の認証装置を、加入者の記録を移動無線網（ＰＬＭＮ）の加入者データベース（ＨＬＲ）で行うことなしに、インターフェース（ＤＳＳ１＋）によって準備しかつインターフェース（ＤＳＳ１＋）を介し別の通信網に伝送し、

－別の通信網（ＣＮ）の加入者のための認証及び／又は情報のコード化を、移動無線網（ＰＬＭＮ）によって受信された保護パラメータに基づいて前記別の通信網（ＣＮ）で実行することを特徴とする方法。

【請求項２】　それぞれの保護パラメータ（ＳＰＡＲ）を準備する移動無線網（ＰＬＭＮ）の認証装置（ＡＣ）を、加入者識別（ＩＭＳＩ）によって検出し、該加入者識別（ＩＭＳＩ）が、加入者局（ＵＰＴＳ，ＤＭ）によって加入者識別モジュール（ＳＩＭ）から読みとられかつインターフェース（ＤＳＳ１＋）を介し送信されることを特徴とする、請求項１に記載の方法。

【請求項３】　別の通信網（ＣＮ）に到達した保護パラメータ（ＳＰＡＲ）を、付加的に加入者データベース（ＤＢ）に記録することを特徴とする、請求項１又は２に記載の方法。

【請求項４】　加入者データベース（ＤＢ）が別の通信網（ＣＮ）に登録された加入者のホーム・データベースであることを特徴とする、請求項３に記載の方法。

【請求項５】　インターフェース（ＤＳＳ１＋）を介し保護パラメータ（ＳＰＡＲ）のそれぞれ１つ又は複数のセットを要求して伝送し、かつ保護パラメータの別のセットを使用する前に、加入者認証及び／又はコード化を行うことを特徴とする、請求項１－請求項４のいづれか１項に記載の方法。

【請求項６】　移動無線網（ＰＬＭＮ）がＧＳＭ基準に基づくセル状の移動無線網であり、該移動無線網によって別の通信網（ＣＮ）の加入者のためのＧＳＭ保護パラメータ（ＳＲＥＳ，ＲＡＮＤ，ＫＣ）を準備することを特徴とする、請求項１－請求項５のいづれか１項に記載の方法。

2

【請求項７】　別の通信網（ＣＮ）の加入者のための無線加入者局（ＤＭ）を使用する場合には、保護アルゴリズムが、無線加入者局と基地局（ＢＳ）との間で空気を介し送信されるべき情報をコード化するための手段を有していることを特徴とする、請求項１－請求項６のいづれか１項に記載の方法。

【請求項８】　加入者を認証するための及び／又は情報をコード化するための装置であって、

移動加入者が、加入者局に含まれた加入者識別モジュール（ＳＩＭ）によって移動無線網に対し識別され、かつ移動無線網（ＰＬＭＮ）の少なくとも１つの加入者データベースに記録されて認証装置（ＡＣ）に登録され、該認証装置（ＡＣ）から加入者データを保護するため、移動加入者に対しそれぞれ保護パラメータ及び保護アルゴリズムが準備可能である形式のものにおいて、

－移動無線網（ＰＬＭＮ）がインターフェース（ＤＳＳ１＋）を介して別の通信網（ＣＮ）に接続されており、別の通信網の加入者が、加入者局（ＵＰＴＳ，ＤＭ）の加入者識別モジュール（ＳＩＭ）によって識別されかつ少なくとも別の通信網（ＣＮ）の加入者データベース（ＤＢ）に記録されており、

－別の通信網（ＣＮ）には、別の通信網（ＣＮ）の記録された加入者のための保護パラメータ（ＳＰＡＲ）をインターフェース（ＤＳＳ１＋）を介して要求する手段（ＰＢＸ）が設けられており、かつ移動無線網（ＰＬＭＮ）のそれぞれの認証装置（ＡＣ）には、保護パラメータ（ＳＰＡＲ）を準備する手段が設けられており、更に移動無線網には、移動無線網（ＰＬＭＮ）の加入者データベースに加入者の記録を行うことなしに、保護パラメータ（ＳＰＡＲ）をインターフェース（ＤＳＳ１＋）を介し別の通信網（ＣＮ）に送信する手段（ＭＳＣ）が設けられており、

－別の通信網（ＣＮ）の加入者のための認証及び／又は情報のコード化を、移動無線網（ＰＬＭＮ）によって受信された保護パラメータに基づいて実行する手段（ＰＢＸ）が別の通信網に設けられている

ことを特徴とする装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、請求項１及び請求項８の上位概念に記載の、加入者を認証するための及び／又は情報をコード化するための方法及び装置に関する。

【０００２】

【従来の技術】テレコンレポート（ｔｅｌｃｏｍ　ｒｅｐｏｒｔ）１６巻（１９９３）、６号、３２６頁から３２９頁までの論文「汎欧州移動通信における安全第１」

（Ｓａｆｅｔｙ　Ｆｉｒｓｔ　ｂｅｉ　ｅｕｒｏｐａｗｅｉｔｅｒ　Ｍｏｂｉｌｋｏｍｍｕｎｉｃａｔｉｏｎ）によれば、国際ＧＳＭ基準（Ｇｌｏｂａｌ　Ｓｙｓｔｅｍ　ｆｏｒ　Ｍｏｂｉｌｅ　Ｃｏｍｍｕｎｉｃａｔｉｏｎ）に基づくセル・ディジタル移動無線網の移動加入者のために、個人的な加入者情報に不正にアクセスしたり悪用したりすることから、加入者データを保護するための方法及び装置が公知である。その際国境を越えて異なる事業者の通信網内で通信することができる移動加入者は、それぞれの通信網に対し、無線加入局内として特徴づけられた加入者識別モジュール（Ｓｕｂｓｃｒｉｂｅｒ　Ｉｄｅｎｔｉｔｙ　Ｍｏｄｕｌｅ）によって識別される。移動加入者はＳＩＭカードの受領後認証装置（Ａｕｔｈｅｎｔｉｆｉｃａｔｉｏｎ　Ｃｅｎｔｅｒ）に登録され、該装置から移動加入者のデータを保護するために、それぞれ安全パラメータ及び安全アルゴリズムが準備されている。この目的のために認証装置が１つの安全ユニット（Ｓｅｃｕｒｉｔｙ　Ｂｏｘ）を有しており、該安全ユニットに安全アルゴリズムが準備されている。更に伝送のための情報をコード化するための方法（ｃｉｐｈｅｒｉｎｇ）も公知である。

【０００３】安全性が極めて重要であるためＧＳＭ保護手段、特に保護パラメータ及び保護アルゴリズムは、１つの共通な取り決め（Ｍｅｍｏｒａｎｄｕｍ　ｏｆ　Ｕｎｄｅｒｓｔａｎｄｉｎｇ）に基づき、州を越えて延びている移動無線網基準に接続された通信網事業者と、インフラストラクチャー製造者とだけがアクセスできるようになっている。従ってこの保護手段は、移動無線網内だけで使用可能であって、別の通信網、例えば専用網（Ｃｏｒｐｏｒａｔｅ　Ｎｅｔｗｏｒｋｓ）内では使用することができない。またＧＳＭ基準と別の機能基準、例えば、ＤＥＣＴ基準（Ｄｉｇｉｔａｌ　Ｅｎｈａｎｓｅｄ　Ｃｏｒｄｌｅｓｓ　Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎ）との間では使用不可能であり、又はたとえＧＳＭ移動無線網の事業者と別の通信事業者との間に加入者移動性（Ｒｏａｍｉｎｇ）の保護に関する通信網間の共通な取り決めが存在していても、１つの共通な通信網（Ｕｎｉｖｅｒｓａｌ　Ｐｅｒｓｏｎａｌ　Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎ，ＵＰＴ）内で使用することは、もちろん不可能である。従ってＧＳＭ基準に保護された移動無線網の間だけに取り決めが存在しうるようになっているか、又は異なった機能基準の通信網での使用は両通信網の加入者データベースの二重加入者登録によってだけ可能である、つまり異なった認証方法によってだけ可能であるようになっている。

【０００４】

【発明が解決しようとする課題】本発明の課題は、加入者を認証するための及び／又は情報をコード化するための方法及び装置を提供し、それによって保護手段が、それぞれ移動無線網に接続された別の通信網においても可能な限りわずかなコストで使用することができるようにすることである。

【０００５】

【課題を解決するための手段】本発明では、方法に関しては請求項１に記載の特徴によって、装置に関しては請求項８に記載の特徴によって、それぞれ上記課題を解決することができた。

【０００６】保護パラメータには、別の通信網の加入者のために移動無線網から両通信網にわたり接続されたインターフェースが準備されていて、移動無線網におけるこれらの加入者のための加入者登録が、移動無線網の少なくとも１つの加入者データベースで行われなくても良いようになっている。その場合別の通信網の加入者は、それぞれ加入者識別モジュールによって識別されかつ少なくとも別の通信網の加入者データベースに記録される。別の通信網に記録された加入者のための保護パラメータは、インターフェースを介して要求することができ、移動無線網の認証装置によって準備されかつインターフェースを介して別の通信網に伝送される。移動無線網の加入者データベースへの加入者の記録は行われないままである。これによって、移動無線網の移動加入者呼び出し番号を配信しなくても良いようになり、別の通信網の加入者の管理を行う必要がないという極めて大きな利点が得られる。移動無線網から配信されて別の通信網に受信された保護パラメータに基づいて、別の通信網に登録された加入者のための加入者認証及び／又は情報のコード化が行われる。別の通信網、例えば、ローカル局装置を備えた専用網は、このような形式で、加入者データへの不正なアクセス及び個人的な加入者データの不正な使用及び／又は情報のコード化に対する保護のための対策を自主的に展開することができる。

【０００７】しかもこれによって、移動無線網が（保護パラメータの伝送を別にして）影響を受けないようになっており、かつ別の通信網が、別の通信網における保護パラメータを改定するための極秘保護アルゴリズムを実行する必要がないようになっている。その際有利には、保護パラメータの別のセットを準備するための移動無線網への新しい要求が別の通信網によって開始される前に、先ず保護パラメータの少なくとも１つのセットがインターフェースを介し要求されて伝送され、かつ加入者認証及び情報のコード化が行われるようになっている。

【０００８】つまり加入者認証のための、特に基地局と参加者無線局との間で空気を介し伝送される情報のコード化のための、保護パラメータ及び保護アルゴリズムの使用は、別の通信網（例えば、ＤＥＣＴ基準に指示された専用網）を介しての加入者の通信の際にも、また加入者が滞在地を別の通信網の領域から移動無線網の供給領域に変えようとする場合の加入者の通信の際にも、また加入者が滞在地を別の通信網の領域から移動無線網の供給領域に変えようとする場合の加入者の通信の際にも、

5

これを変換することができるようになっている。

【０００９】

【発明の実施の形態】次に本発明を、図に示された実施形態に基づいて詳しく説明する。

【００１０】図１には、インターフェースＤＳＳ１＋を介し移動無線網ＰＬＭＮに、例えば、ＧＳＭ基準に基づく移動無線網で接続されている専用網ＣＮで加入者の認証及び情報のコード化を行うためのブロック図が示されている。セル上に構築されたディジタル移動無線網ＰＬＭＮは、公知のように、無線技術的な部分装置と接続技術的な部分装置とを有している。その際、ホーム加入者データベース（ホーム・レジスタ）で接続技術的な部分装置のビジター加入者データベース（ビジター・レジスタ）の滞在地に依存して登録された移動加入者の無線局が、エアインターフェースを介して、無線技術的な部分装置の多数の基地送信／受信局の内のそれぞれ１つに接続されており、またこれとは逆に接続されている。基地送信／受信局は多数の無線セルに作用を及ぼしており、該無線セルから無線供給のための移動無線網ＰＬＭＮが、可能な限り多くの加入者を１つにまとめている。

【００１１】接続技術的な部分装置は、接続に関連する移動特性的な機能を実現するための無線技術的な部分装置に接続されている。接続技術的な部分装置は、付属のビジター・レジスタＶＬＲを備えた多数の移動接続箇所ＭＳＣを有していて、１つの移動接続箇所ＭＳＣにそれぞれ役立っている供給領域の加入者データが、実際に滞在する加入者に分散されて一時的に供給されうるようになっている。つまり移動加入者のデータは、該データがそれぞれの受け持ち供給領域内に位置する限り、移動無線網ＰＬＭＮの分散された加入者データとして機能するビジター・レジスタＶＬＲにだけ保存されるようになっている。ビジター・レジスタＶＬＲの外に移動無線網ＰＬＭＮは、少なくとも一つの図示されていないホーム・レジスタＨＬＲを有している。その際総ての移動加入者の総ての加入者データは、登録の期間の間移動無線網ＰＬＭＮに集中して供給される。

【００１２】認証装置ＡＣはホーム・レジスタＨＬＲに接続されていて、固有のプロセッサと固有の運転装置とを備えた保護ユニット（Ｓｅｃｕｒｉｔｙ　Ｂｏｘ）を有している。認証装置ＡＣには、移動加入者が加入者に配分された移動加入者識別ＩＭＳＩによって登録されており、その際ＳＩＭカードの準備に基づく秘密な加入者符号ＫＩも記憶される。ＳＩＭカードは加入者識別モジュールＳＩＭであり、該カードＳＩＭによって加入者は移動通信網ＰＬＭＮに対し識別される。

【００１３】加入者識別モジュールＳＩＭを用いて加入者を識別した後、移動加入者の通信網アクセス認可を検査するための加入者認証が行われる。この目的のために認証装置ＡＣには保護パラメータＳＰＡＲが準備されていて、所定の保護アルゴリズム（例えば、国際ＧＳＭ基準に基づいて規定された保護アルゴリズムＡ３／Ａ８）のための入りロパラメータとして使用されており、該保護アルゴリズムは、他方では、認証のための保護パラメータ（後で説明する、例えば、ＳＲＥＳ）ないしは情報をコード化するための保護パラメータ（後で説明する、例へば、ＫＣ）を出発パラメータとして供給しうるようになっている。しかし州にまたがるＧＳＭ移動無線網の事業者は、この保護アルゴリズムに接続されていなくて、独自の保護アルゴリズムを提供することができるようになっている。

6

【００１４】認証装置ＡＣの保護ユニットには、乱数（ＲＡＮＤ）と、記憶されたパラメータＩＭＳＩ及びＫＩとを使用した保護アルゴリズムＡ３の結果として、１つの信号（ＳＲＥＳ、サインされた応答）が供給される。同じように内方に提供された保護アルゴリズムＡ３に基づく加入者及び記憶されたパラメータＩＭＳＩ，ＫＩに基づいて信号（ＳＲＥＳ、サインされた応答）を形成する。この両信号が移動無線網ＰＬＭＮの通信網装置によって、有利には移動接続箇所ＭＳＣによって、自己同一性に関し相互に比較される。両信号が一致した場合には加入者認証が効果的に実行される。認証の間保護アルゴリズムＡ８に基づく加入者識別モジュールＳＩＭでは情報をコード化するための符号（ＫＣ）が算出される。移動無線網ＰＬＭＮの個々の装置が通信することができるように中央プロッティング装置ＣＣＳ７（プロッティング装置番号７）が設けられており、該プロッティング装置は、移動性に関連した機能を処理するための、移動機能特性を備えたユーザ部分ＭＡＰを有している。

【００１５】専用網ＣＮは少なくとも１つのローカル局装置ＰＢＸを有し、該ローカル局装置ＰＢＸに加入者は、加入者局ＵＰＴＳを介して有線接続されているか、又は無線加入者局ＤＭ、例えば、ＧＳＭ基準及びＤＥＣＴ基準に適合した双対モード加入者局と、基地局ＢＳとを介して接続されている。その際加入者局ＵＰＴＳは、有線接続された加入者の一般的な個人通信及び／又は移動加入者に役立つ通信網（一般的な個人通信、ＵＰＴ）をバックアップする。両加入者局ＵＰＴＳ，ＤＭは共通であって、専用網ＣＮの加入者が、加入者局に含まれた又は加入者局内に挿入された加入者識別モジュールＳＩＭによって、通信網に対して識別されうるようになっている。

【００１６】加入者識別モジュールＳＩＭは、加入者のために加入者識別ＩＭＳＩと、秘密な加入者符号ＫＩが、例えば、実行される保護アルゴリズムＡ３に基づいて加入者認証のためにだけ使用される一方で、加入者識別ＩＭＳＩは、移動無線網ＰＬＭＮの認証装置ＡＣの確定に役立っており、該認証装置ＡＣによって、認証のための保護パラメータＳＰＡＲ及び／又は専用網ＣＮの加入者のコード化が準備されるようになっている。専用網は、例えば、多数の位置を備えた企業通信網（Ｃｏｒｐ

ｏｒａｔｅ　Ｎｅｔｗｏｒｋ）から成っており、該位置は相互にネットワーク化されており、かつローカル局装置ＰＢＸに加入者は、導線又は無線通路を介し、例えば、ＤＥＣＴ無線装置の接続によって接続されている。

【００１７】ローカル局装置ＰＢＸはそれぞれ１つの加入者データベースＤＢを有し、該データベースＤＢには、それぞれ登録された加入者のデータが記憶されている。加入者データには、例えば、インターフェースＤＳＳ１＋を介して到達可能である移動接続箇所ＭＳＣと、加入者番号ＳＮＲと、認証装置ＡＣを探索するための、加入者識別モジュールＳＩＭから加入者局ＵＰＴＳ，ＤＭに受信される加入者識別ＩＭＳＩと、加入者によりそれぞれ利用可能である通信サービスを確認するためのサービス手段ＳＰＲＯと、認証装置ＡＣから提供される保護パラメータＳＰＡＲとが含まれており、該保護パラメータＳＰＡＲに基づいて専用網ＣＮには、認証手順及び／又はコード化手段が自主的に展開されるようになっている。

【００１８】ローカル局装置ＰＢＸと移動接続箇所ＭＳＣとの間に位置するインターフェースＤＳＳ１＋を介してインターフェース・プロトコルが使用されており、該プロトコルによって、移動性及び保護性に特有な機能の影響下で保護パラメータＳＰＡＲの交換を行うことができるようになっている。インターフェースＤＳＳ１＋は、ローカル局装置ＰＢＸから移動接続箇所ＭＳＣに接続するために、例えば、１つのプロトコルを利用していて、保護パラメータＳＰＡＲを伝送するための情報分だけ拡大されている。これによって、例えば、保護アルゴリズムと、準備された専用網ＣＮの保護パラメータとを導くことができ、かつ無線加入者局ＤＭ及び基地局ＢＳの間で空気を介して送信されるべき情報（例えば、言語及び日付）をコード化するための手段を使用することができるようになっている。このためエアインターフェースのための特別な符号（ＫＣ）が必要であり、該符号（ＫＣ）は、保護パラメータＳＰＡＲの部分として移動無線網から要求されかつ認証装置ＡＣによって準備され又はインターフェース　ＤＳＳ１＋を介して受信されうるようになっている。

【００１９】図２には、移動無線網から保護パラメータＳＰＡＲを伝送することによって、専用網ＣＮに登録された加入者を認証するための経過が示されている。しかもこの場合は加入者記録を、移動無線網ＰＬＭＮのホーム・レジスタＨＬＲで行わなくてもよいようになっている加入者局ＤＭ及びＵＰＴＳで加入者の識別を行った後、特に加入者識別ＩＭＳＩを含む情報ＬＵＲがローカル局装置ＰＢＸに送信され、該ローカル局装置ＰＢＸによって加入者は、加入者データベースＤＢに加入者データを記録することにより登録される。滞在地登録が初めて必要である場合、又は別のローカル局装置の領域内には入り込んだ際滞在地登録が必要であるような場合には、情報ＬＵＲ（位置更新要求）が加入者局から常に送信される。

【００２０】専用網ＣＮのローカル局装置ＰＢＸから加入者識別ＩＭＳＩを備えた情報箇所ＳＰＲが、情報ユニットとして移動接続箇所ＭＳＣのための図１のインターフェースを介し、専用網ＣＮに登録された加入者を認証するための及び／又は保護パラメータを伝送するための要求を信号伝送する。その後移動接続箇所ＭＳＣは、加入者識別ＩＭＳＩを備えた情報ＳＡＵＩを対応する認証装置ＡＣのための情報ユニットとして送信する。情報ＳＡＵＩ（送信認証情報）と一緒に、認証装置で計算されて準備された保護パラメータＳＰＡＲが要求される。その際保護パラメータＳＰＡＲの要求は、通常、識別ＩＭＳＩを含む加入者記録が行われることなしに遂行される。また移動加入者呼び出し番号（ＭＳＩＳＤＮ）の設定も行われない。このため専用網ＣＮの加入者は、加入者に所属するローカル局装置ＰＢＸにおいてだけ加入者として登録される一方で、この加入者のホーム・レジスタＨＬＲには存在していなくて、加入者に対し保護パラメータだけが、認証装置ＡＣによって通過されたデータとして保管されかつホームローカル局装置として加入者を登録したローカル局装置ＰＢＸの方に送信される。

【００２１】このため加入者識別モジュールＳＩＭが、別の通信網、例えば、専用網ＣＮの通信網事業者に出力され、該モジュールＳＩＭは、対応する加入者データベースに、この例ではローカル局装置ＰＢＸの加入者データベースに、加入者を記録するためにだけ役立っている。通信網事業者又はサービス提供者によって加入者局の利用者に出力されたＳＩＭカードが、加入者によって無線加入者局ＤＭ内又は加入者局ＵＰＴＳ内に挿入されて、それぞれの通信網に対し識別されうるようになっている。この実施形態では、認証装置ＡＣにより専用網ＣＮへの加入者の通信網アクセスのために必要である保護パラメータとして、乱数ＲＡＮＤと、無線伝送の間に情報をコード化するための符号ＫＣと、加入者識別モジュールＳＩＭの認可検査のために通信網に対して必要である信号ＳＲＥＳ（サイン応答）とが準備されて、移動接続箇所ＭＳＣへ情報ＲＳＡＵＩ（結果送信認証情報）が発信されうるようになっている。

【００２２】その際、保護パラメータの１つ又は複数のセットが準備されており、該保護パラメータは、専用網ＣＮにおいて先ず認証のために加入者によって処理され、その後で別のセットが保護パラメータによって要求されるようになっているので有利である。つまり保護パラメータの多くの異なったセットを移動無線網の認証装置から呼び出すことができ、引き続き専用網において、この例では、付属の加入者データベースＤＢを備えたローカル局装置ＰＢＸによって前記セットが処理される。移送接続箇所ＭＳＣは、情報ＲＳＡＵＩの受信後情報ＲＳＰ（Ｒｅｓｕｌｔ　Ｓｅｃｕｒｉｔｙ　Ｐａｒａｍｅ

ｔｅｒ）内に届いたパラメータＲＡＮＤ，ＳＲＥＳ，ＫＣをインターフェースを介し専用網に送信し、ここで前記パラメータは、ローカル局装置ＰＢＸの加入者データベースに保護パラメータＳＰＡＲとして記憶される。

【００２３】この手順は、認証装置ＡＣが前もって要求された保護パラメータの１つのセットを準備して伝送するその度ごとに繰り返される。ローカル局装置ＰＢＸに登録された専用網ＣＮの加入者のための加入者認証は、ローカル局装置ＰＢＸによって乱数ＲＡＮＤを備えた情報ＡＵＲが情報ユニットとしてそれぞれの加入者局ＤＭ又はＵＰＴＳに対し発信されることによって、引き続き自動的に行われる。情報のコード化のために特別な符号ＫＣが、ローカル局装置ＰＢＸに接続された基地局か、又はコード化された利用情報又は信号化情報を送信するための加入者局か、のどちらかによって利用されている。

【００２４】ローカル局装置ＰＢＸは、認証に対する希望を情報ＡＵＲを用いて信号化する。この希望は、信号ＳＲＥＳを有する情報ＲＡＵの呼び出し装置を備えた加入者局ＤＭ又はＵＰＴＳによって情報ユニットとして応答される。届いた乱数ＲＡＮＤを基礎にしてそれぞれの加入者局は、ＳＩＭカードの準備に基づく秘密加入者コードを用いて信号ＳＲＥＳが、ローカル局装置ＰＢＸによって加入者データベースＤＢに記憶された信号ＳＲＥＳと同一であるかどうかを比較する。両信号が一致した場合には、加入者の通信網で保護アルゴリズムを実行する必要なしに専用網ＣＮに登録された加入者の認証を効果的に行うことができる。移動無線網ＰＬＭＮの移動加入者と、別の通信網ＣＮの加入者とのための別個の認証手順を省くことができる。

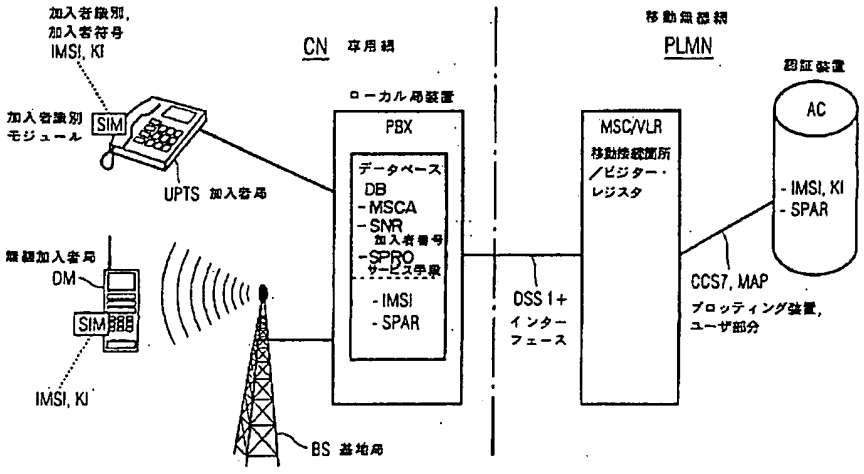
【００２５】保護パラメータが、この実施形態では専用網ＣＮの加入者の認証のためのＧＳＭ保護パラメータが、専用網の加入者のための加入者記録を移動無線網の加入者データベースで行うことなしに、前もって要求されて伝送される。この実施形態は、ＧＳＭ保護アルゴリズムに基づいて処理されるＧＳＭ保護パラメータを準備することに関しているが、別の通信網の加入者の認証のための、又は情報のコード化のための、別の保護パラメータ及び保護アルゴリズムも本発明の対象になっている。保護パラメータの伝送のためには、移動無線網と別の各通信網の間にインターフェースプロトコルによるインターフェース接続を行う必要がある。

【図面の簡単な説明】

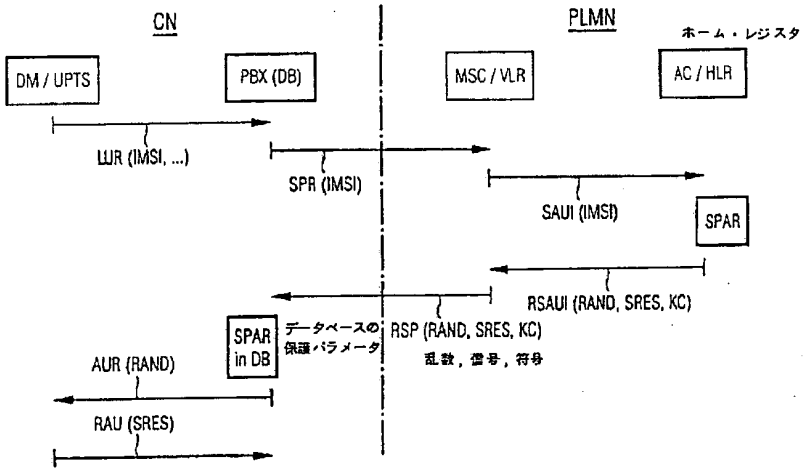
【図１】移動無線網に接続された専用網における加入者認証のブロック図である。

【図２】専用網と移動無線網との間で加入者を認証するための情報の流れ図である。

【図１】



【図２】


CN
PLMN
ホーム・レジスタ
DM / UPTS
PBX (DB)
MSC / VLR
AC / HLR
LUR (IMSI, ...)
SPR (IMSI)
SAUI (IMSI)
SPAR
RSAUI (RAND, SRES, KC)
SPAR in DB
データベースの保護パラメータ
RSP (RAND, SRES, KC)
乱数，暗号，符号
AUR (RAND)
RAU (SRES)